УДК 004.056.55

В. А. ПОНОМАР

ОСОБЛИВОСТІ ТА ПРОБЛЕМАТИКА СТВОРЕННЯ КРИПТОСИСТЕМ, ЗАСНОВАНИХ НА ВИКОРИСТАННІ ІЗОГЕНІЙ ЕЛІПТИЧНИХ КРИВИХ

Вступ

З появою квантового комп'ютера криптостійкість існуючих криптографічних систем значно зменшиться, бо існуючі системи для методів квантового криптоаналізу мають лише поліноміальну складність. Тому виникає необхідність створення систем на основі криптографічних перетворень, що є стійкими до квантового криптоаналізу, тобто будуть мати експоненційну чи субекспоненційну складність. Одним з таких методів є використання ізогеній. Ізогенія – це відображення точок однієї кривої в іншу. Для криптосистем з відкритим ключем планується, що сама ізогенія – це особистий ключ, а крива, до якої вона веде, – відкритий. Тому стійкість залежить від складності розрахунку ізогенії між двома відомими кривими. Ця складність має експоненційний характер.

1. Загальні відомості про ізогенії

Ізогенія – це раціональне відображення $\varphi: E_1(K) \to E_2(K)$, де $E_1(K)$ та $E_2(K)$ є еліптичними кривими, а $\varphi(P_\infty) = P_\infty$[1, 2]. Нульова ізогенія – це ізогенія, що відображає усі точки однієї кривої у точку на нескінченності іншої. Ядром ізогенії є

$$Ker(\varphi) = \{K_i \in E_1\};\ \varphi(K_i) = P_\infty.$$

Ізогенії ініціюють відображення полів функцій на кривих. Степінь розширення $(K(E_1): \varphi * K(E_2))$ називається степінню ізогенії.

Для ізогенії $\varphi: E_1(K) \to E_2(K)$ існує дуальна ізогенія $\hat{\varphi}: E_2(K) \to E_1(K)$, така, що $\hat{\varphi}\varphi = [l]$, де l – множення точки кривої E_1 на число l, аналогічно $\varphi\hat{\varphi} = [l]$, де l – множення точки кривої E_2 на число l. Дуальні ізогенії мають однакову степінь.

У випадку алгебраїчно замкненого поля операція множення точки на число l задає ендоморфізм еліптичної кривої з ядром l^2 точок. Оскільки ізогенія відповідає квадратному кореню з операції множення на l, то ядро ізогенії складається з l точок порядку l , що створюють циклічну групу (однією з них є точка P_∞).

Ізогенії складних степенів можуть використовуватися, як композиція ізогеній простих степеней.

Властивості ізогеній, що використовуються при створенні криптосистем:

$$\gamma(\varphi(A)) = \varphi(\gamma(A)) = \gamma\varphi(A); \quad (1)$$

$$k * A_\varphi = \varphi(k * A). \quad (2)$$

2. Знаходження ізогеній по ядру

Для знаходження ізогенії $\varphi: E_1(K) \to E_2(K)$ з заданим ядром використовується формула Велу [3, 4].

Для еліптичної кривої, що задана формулою Вейєрштрасса:

$$E_1: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (3)$$

Нехай C – группа точок еліптичної кривої, що буде ядром ізогенії. Тоді:

1. Формуємо набір точок S:

- виключаємо з С точку на нескінченності;
- нехай C_2 – усі точки C, в яких координата y дорівнює нулю, а R – усі інші точки C;
- розділимо точки набору R на R_+ та R_- таким чином, що для кожної точки P, що належить R_+ , $-P$ належить R_-;
- $S = R_+ \cup C_2$.

2. Для кожної точки $Q \in S$ виконуємо наступні обчислення:

$$g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q; \quad (4)$$

$$g_Q^y = -2y_Q - a_1x_Q - a_3; \quad (5)$$

$$v_Q = \begin{cases} g_Q^x, & 2Q = \infty \\ 2g_Q^x - a_1g_Q^y, & 2Q \neq \infty \end{cases}; \quad (6)$$

$$u_Q - (g_Q^y)^2; \quad (7)$$

$$v = \sum_{Q \in S} v_Q; \quad (8)$$

$$w = \sum_{Q \in S} (u_Q + x_Q v_Q). \quad (9)$$

3. Розраховуємо формулу еліптичної кривої $E_2(K)$:

$$A_1 = a_1; \quad (10)$$

$$A_2 = a_2; \quad (11)$$

$$A_3 = a_3; \quad (12)$$

$$A_4 = a_4 - 5v; \quad (13)$$

$$A_6 = a_6 - (a_1^2 + 4a_2)v - 7w; \quad (14)$$

$$E_2: y^2 + A_1xy + A_3y = x^2 + A_2x^2 + A_4x + A_6. \quad (15)$$

4. Розраховуємо координати точки $(x_\varphi, y_\varphi) = \varphi(x,y)$:

$$x_\varphi = x + \sum_{Q \in S}\left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}\right); \quad (16)$$

$$y_\varphi = y - \sum_{Q \in S}\left(u_Q\frac{2y + a_1x + a_3}{(x - x_Q)^3} + v_Q\frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - g_Q^xg_Q^y}{(x - x_Q)^2}\right) \quad (17)$$

Отримані формули на кроці 4 й будуть ізогенією з заданим ядром.

Оскільки в криптографії еліптичних кривих, прийнято використовувати спрощену формулу Вейєрштрасса, то й ми приведемо до прийнятого вигляду.

$$E_1: y^2 = x^3 + a_4x + a_6 \quad (18)$$

Нехай C – группа точок еліптичної кривої, що буде ядром ізогенії. Тоді:

1. Формуємо набір точок S:

а) Виключаємо з С точку на нескінченності.

б) Нехай C_2 – усі точки C, в яких координата y дорівнює нулю, а R – усі інші точки C.

в) Розділимо точки набору R на R_+ та R_-, таким чином, що для кожної точки P, що належить R_+, $-P$ належить R_-.

г) $S = R_+ \cup C_2$.

2. Для кожної точки $Q \in S$ виконуємо обчислення:

$$g_Q^x = 3x_Q^2 + a_4; \quad (20)$$

$$g_Q^y = -2y_Q; \quad (21)$$

$$v_Q = \begin{cases} g_Q^x, & 2Q = \infty \\ 2g_Q^x, & 2Q \neq \infty \end{cases}; \quad (22)$$

$$u_Q = (g_Q^y)^2; \quad (23)$$

$$v = \sum_{Q \in S} v_Q; \quad (24)$$

$$w = \sum_{Q \in S} (u_Q + x_Q v_Q). \quad (25)$$

3. Розраховуємо формулу еліптичної кривої $E_2(K)$:

$$A_4 = a_4 - 5v; \quad (26)$$

$$A_6 = a_6 - 7w; \quad (27)$$

$$E_2: y^2 = x^2 + A_4x + A_6. \quad (28)$$

4. Розраховуємо координати точки $(x_\varphi, y_\varphi) = \varphi(x,y)$:

$$x_\varphi = x + \sum_{Q \in S}\left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}\right); \quad (29)$$

$$y_\varphi = y - \sum_{Q \in S}\left(u_Q\frac{2y}{(x - x_Q)^3} + v_Q\frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^xg_Q^y}{(x - x_Q)^2}\right). \quad (30)$$

3. Вибір еліптичних кривих для криптографічних систем на основі ізогеній

Складність знаходження ізогенії за її ядром, за умов використання цього алгоритма, становить $O(l^3)$ [3, 4], де l – порядок ізогенії. Щоб зменшити складність обчислення пропонується використання суперсингулярних кривих, що дозволить розбивати ізогенію на композицію ізогеній малого порядка. Наприклад обчислення ізогенії порядка 2^{64} має складність 2^{192}, а якщо її розбити на композицію ізогеній порядка 2, складність обчислення фінальної ізогенії становить $64 * 2^3 = 2^9$. Оскільки наші криптосистеми будуть засновані на використанні ізогеній, то вразливість суперсингулярних кривих до вирішення задачі знаходження дискретного логарифму не впливає на стійкість криптографічної системи на основі ізогеній при використанні таких кривих.

За теоремою Сільвермана [2, 3] кількість суперсингулярних еліптичних кривих над полями характеристики p становить $\frac{p+1}{12} + 1$. Пропонується використовувати квадратичні розширення полів F_{p^2}, що дозволить досить легко за алгоритмом Брокера будувати суперсингулярні криві [1].

4. Проблема створення криптосистем з відкритим ключем на ізогеніях еліптичних кривих та складність криптоаналізу

Планується, що в криптосистемах на ізогеніях еліптичних кривих при спільному параметрі ЕК E_1 таємним ключем буде ізогенія $\varphi: E_1(K) \to E_2(K)$, а ЕК E_2 – відкритим ключем. На рис. 1 зображена спрощена схема криптоперетворень на ізогеніях ЕК [3].

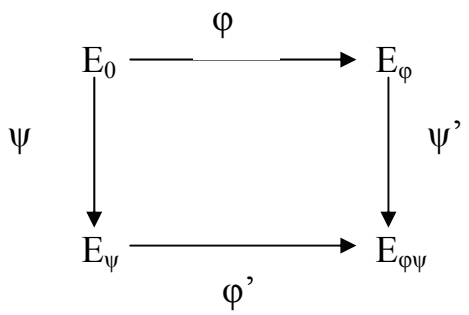

Рис. 1. Спрощена схема криптоперетворень на ізогеніях ЕК

На схемі E_0, E_φ, E_ψ, $E_{\varphi\psi}$ – еліптичні криві, φ, ψ, φ’, ψ’ – ізогенії, причому $Ker(\varphi') = \psi(Ker(\varphi))$ та $Ker(\psi') = \varphi(Ker(\psi))$. Проблема використання ізогеній в криптосистемах з відкритим ключем полягає в тому, що якщо криптоаналітику відома пара (ψ, φ’) чи (φ’, ψ’), він може знайти φ – особистий ключ [5]. Це витікає з того, що пошук зворотної ізогенії має низьку складність. Для цього на еліптичній кривій обирається точка, що не належить ядру ізогенії та має порядок, який дорівнює порядку ізогенії. Ця точка відображається через лізогенію, і з її відображення будується нова ізогенія, що веде до еліптичної кривої, яка ізоморфна до початкової, обчислення відповідного ізоморфізму є простою задачею. Далі наведено алгоритм відновлення секретної ізогенії через знання її відображення через відкриту ізогенію.

1. Нехай криптоаналітику відома пара (ψ, φ’). Тоді він будує зворотню ізогенію $\hat{\psi}$, $Ker(\varphi) = \hat{\psi}(Ker(\varphi'))$.

2. Нехай криптоаналітику відома пара (φ’, ψ’). Тоді він будує зворотні ізогенії $(\hat{\varphi'}, \hat{\psi'})$, далі знаходить $Ker(\hat{\psi}) = \hat{\varphi'}(Ker(\hat{\psi'}))$, після цього можна знайти $Ker(\varphi) = \hat{\psi}(Ker(\varphi'))$.

З цього випливає, що якщо криптоаналітику стають відомі сусідні ребра ромбічної структури графів ізогеній, то, незалежно від їх направленості, він може відновити усю схему криптосистеми і встановити невідомі ізогенії. Тому в криптосистемі повинне зберігатися в таємниці не лише секретна ізогенія, а й протилежна їй у графі ізогеній. Саме це є однією з основних проблем при побудові схем електронного підпису (ЕП) на ізогенії еліптичних кривих.

Атака на ізогенії полягає в пошуку ізогенії між двома відомими ЕК. Для цього від кожної еліптичної кривої будується дерево ізогеній, доки вийде співпадання в спільній вершині ЕК. Тобто примусове створення другого випадку наведеної вище ситуації, де E_φ, E_ψ – наші початкові еліптичні криві, а $E_{\varphi\psi}$ – спільна вершина. Ця атака називається «зустріч посередині». Побудова ізогеній відразу з двох вершин робиться для того, щоб зменшити складність, бо складність побудови двох ізогеній порядка l/2 менша складності побудови ізогенії порядка l в чотири рази. Складність атаки «зустріч посередині» [3, 5] становить $O(p^{1/4})$ для класичного комп'ютера і $O(p^{1/6})$ для квантового, що має експоненційний характер.

5. Ізогенії на кривих Едвардса

Останнім часом набуває популярності дослідження на тему використання еліптичних кривих Едвардса у криптографії. Перевагою таких ЕК вважається значне збільшення швидкодії. Тому необхідно розглянути можливість використання ізогеній для кривих Едвардса.

Криві Едвардса мають наступний вигляд:

$$E_d: x^2 + y^2 = 1 + dx^2y^2 \quad (31)$$

$$E_{a,d}: ax^2 + y^2 = 1 + dx^2y^2 \quad (32)$$

де $a, d \neq \{0, 1\}$. Рівняння суми точок:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right) \quad (33)$$

Крім того, є відображення кривих Едвардса на криві Вейєрштрасса $E: y^2 = x^3 + 2(a + d)x^2 + (a - d)^2x$:

$$\epsilon: (x, y) \to \left((a - d)\frac{1+y}{1-y}, (a - d)\frac{2(1+y)}{x(1-y)}\right), \quad (34)$$

та зворотнє:

$$\epsilon^{-1}: (x, y) \to \left(\frac{2x}{y}, \frac{x-(a-d)}{x+(a-d)}\right) \quad (35)$$

Для побудови ізогеній можна розглянути два випадки:

1. *Побудова ізогеній порядка 2 на кривих Едвардса.*

Нехай є крива Едвардса E_d та три елемента поля u, o, і такі, що $u^2 = 1 - d$, $o^2 = d$, $i^2 = -1$, тоді існує три ізогенії порядка 2 [6]:

$$\omega_1(x, y) \to \left((u \mp 1)xy, \frac{(u\mp1)y^2 \pm 1}{(u\pm1)y^2 \mp 1}\right) \quad (36)$$

$$\omega_2(x, y) \to \left((iu \pm o)\frac{x}{y}, -\frac{oy^2 \mp iu - o}{oy^2 \pm iu - o}\right) \quad (37)$$

$$\omega_3(x, y) \to \left(i(o \mp 1)\frac{x\left(1-dy^2\right)}{y(1-d)}, \frac{(d\mp o)(oy^2\pm1)}{(d\pm o)(oy^2\mp1)}\right), \quad (38)$$

le $\omega_1: E_u \to E_{u'}$, $\omega_2: E_u \to E_{u''}$, $\omega_3: E_u \to E_{u'''}$, для яких $d' = \left(\frac{u\pm1}{u\mp1}\right)^2$, $d' = \left(\frac{iu\mp o}{iu+o}\right)^2$, $d' = \left(\frac{o\pm1}{o\mp1}\right)^2$.

2. *Побудова ізогеній непарного порядка на кривих Едвардса*.

Нехай F – підгруппа кривої Едвардса $E_{a,d}$ порядка $l = 2s + 1$, точками якого є $\{(0,1), (\pm\alpha_1, \beta_1), \dots, (\pm\alpha_s, \beta_s)\}$. Далі за цим ядром обчислюються наступні значення [6]:

$$A = \prod_{i=1}^{s} \alpha_i ; \quad (39)$$

$$B = \prod_{i=1}^{s} \beta_i ; \quad (40)$$

$$a' = \frac{A^4}{B^4}a^l ; \quad (41)$$

$$d' = A^4B^4d^l . \quad (42)$$

Тоді ізогенія $\omega: E_{a,d} \to E_{a',d'}$ має вигляд:

$$\omega(x, y) = \left(-1^s \frac{x}{A^2}\prod_{i=1}^{s}\frac{\beta_i^2x^2 - \alpha_i^2y^2}{1 - d^2\alpha_i^2\beta_i^2x^2y^2}, \frac{y}{B^2}\prod_{i=1}^{s}\frac{\beta_i^2y^2 - \alpha_i^2x^2}{1 - d^2\alpha_i^2\beta_i^2x^2y^2}\right) \quad (43)$$

Обчислення ізогенії для кривих Едвардса виконується в чотири рази швидше ніж на звичайних кривих, тому використання кривих Едвардса має потенціал для подальшої оптимізації обчислення ізогеній.

Але вимагається дослідження використання кривих Едвардса для криптосистем на основі ізогеній на предмет появи вразливостей. Крім того, якщо збільшується швидкість звичайного обчислення, то і збільшуються швидкі виконання атаки «зустріч посередині». До того ж невідомо, чи буде присутній весь обсяг ізогеній еліптичних кривих на їх відображенні у криві Едвардса, бо якщо кількість можливих ізогеній буде інша, то це можливо буде говорити про збільшення чи зменшення криптостійкості.

6. Схема розподілу ключів Діффі – Хелмана на ізогеніях еліптичних кривих

Загальносистемні параметри [3, 5]: еліптична крива $E_0(F_{p^2})$.

Секретні параметри: елементи поля m, n та ізогенія φ.

Відкриті параметри: точки $P, Q \in E_0$ та крива E_φ .

1. Абонент A формує параметри P_A, Q_A, m_A, n_A. Обчислює точку:

$$G_A = m_A P_A + n_A Q_A \tag{44}$$

G_A є точкою, що породжує групу точок – ядро ізогенії φ_A. За формулою Велу будується ізогенія $\phi_A: E_0 \to E_A$. E_A – відкритий ключ.

2. Абонент B робить аналогічні кроки для параметрів P_B, Q_B, m_B, n_B, G_B, φ_B, E_B .

3. Абоненти A і B обмінюються відкритими параметрами.

4. Абонент A обчислює та надсилає $\varphi_A(P_B)$, $\varphi_A(Q_B)$.

5. Абонент B обчислює та надсилає $\varphi_B(P_A)$, $\varphi_B(Q_A)$.

6. Абонент A обчислює точку:

$$G_{AB} = m_A \varphi_B(P_A) + n_A \varphi_B(Q_A) \tag{45}$$

G_{AB} є точкою, що породжує групу точок – ядро ізогенії φ_{AB}. За формулою Велу будується ізогенія $\phi_{AB}: E_B \to E_{AB}$. E_{AB} – розподілена таємниця.

7. Абонент B обчислює точку:

$$G_{BA} = m_B \varphi_A(P_B) + n_B \varphi_A(Q_B) \tag{46}$$

G_{BA} є точкою, що породжує групу точок – ядро ізогенії φ_{BA}. За формулою Велу будується ізогенія $\phi_{BA}: E_A \to E_{BA}$. E_{BA} – розподілена таємниця.

$$E_{AB} = E_{BA} \tag{47}$$

Загальна схема розподілу ключів зображена на рис. 2.

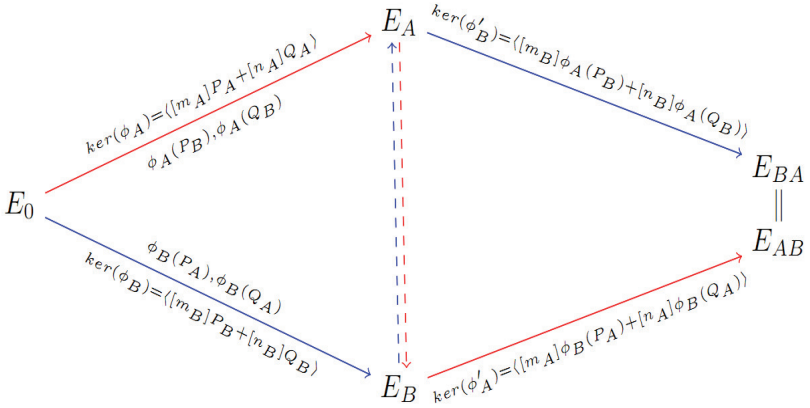

Рис. 2. Схема протоколу Діффі-Хелмана на ізогеніях

Так як кожному з абоненті відомі лише протилежні ізогенії ромбічного графу, то вимога секретності п. 4 виконується.

7. Схема електронного підпису на ізогеніях еліптичних кривих

Схема підпису, що описується в даному розділі, може бути перевірена будь-якою стороною, але для запобігання вразливості, що описана вище, потрібна участь підписувача в інтерактивному режимі. Для того щоб відрізняти неправильний підпис, механізм має можливість підписувачу в інтерактивному режимі довести підробку підпису. На відміну від спрощеної схеми, схема підпису має три проходи – додається ще ізогенія – ключ сесії. Тому зовнішній вигляд графу має форму куба.

Обирається ініціалізуюча еліптична крива $E(F_{p^2})$. На цій кривій обираються пари точок (P_A, Q_A), (P_M, Q_M), (P_C, Q_C) [5]. Точки (P_A, Q_A) будуть використовуватися для генерації ключа підписувача. Точки (P_M, Q_M) для генерації ізогенії, яка буде прив'язана до повідомлення, що підписується. Точки (P_C, Q_C) будуть використовуватися для генерації сесійного ключа для протоколів підтвердження чи спростування підпису.

Підписувач випадково генерує елементи поля m_A, n_A. Отримує ключову точку $K_A = [m_A]P_A + [n_A]Q_A$, точка K_A – точка генерування $Ker(\varphi)$, де ізогенія $\varphi: E \to E_A$ буде секретним ключем підписувача.

Відкриті параметри системи: p, $E(F_{p^2})$, (P_A, Q_A), (P_M, Q_M), (P_C, Q_C) і геш-функція, що використовується.

Відкритий ключ підписувача: E_A, $\varphi(P_C)$, $\varphi(Q_C)$.

Особистий ключ підписувача: m_A, n_A.

Алгоритм підпису полягає в наступному:

Підписувач отримує геш-значення h повідомлення M. Формує точку $K_M = P_M + [h]Q_M$ [5], що буде точкою генерування $Ker(\gamma)$ для ізогенії $\gamma: E \to E_M$.

Формує граф підпису, що зображен на рис. 3, для цього виконує розрахунок ізогеній:

$$\gamma: E \to E_M; \tag{48}$$

$$\gamma_A: E_A \to E_{AM},\ Ker(\gamma_A) = \varphi(Ker(\gamma)); \tag{49}$$

$$\varphi_M: E_M \to E_{AM},\ Ker(\varphi_M) = \gamma(Ker(\varphi)). \tag{50}$$

Крім того, обчислює значення точок ($\varphi_M\gamma(P_C)$, $\varphi_M\gamma(Q_C)$). Ці дві точки, а також значення кривої E_{AM} і буде підписом повідомлення M на ізогенії φ.

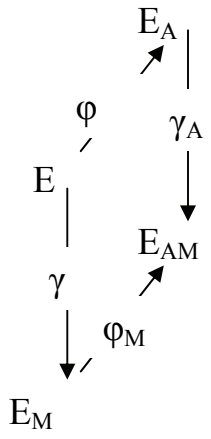

Рис. 3. Граф підпису

Під час виконання протоколу підтвердження підпису необхідно довести правильність кривої E_{AM} без передачі ізогенії, що використовувалася для її створення [5]. Для цього генерується засліплююча ізогенія ε, яка використовується для побудови графу підтвердження підпису, що зображений на рис. 4 і яка передається за спеціальним протоколом підписувачем перевірнику. Ця інтерактивність є основним недоліком використання схеми електронного

підпису на ізогеніях ЕК. Єдина система, в якій можливо не звертати увагу на цей недолік, – це хмара.

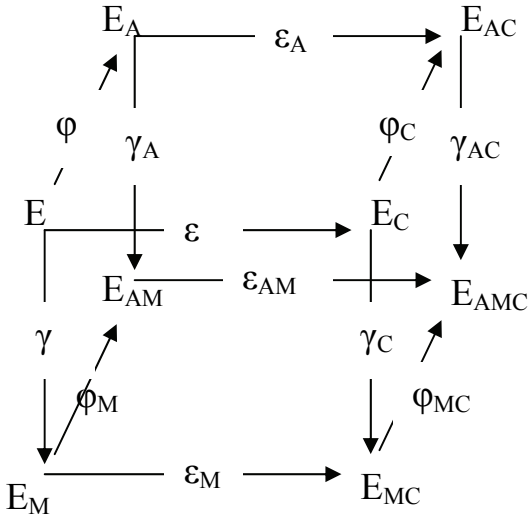

Рис. 4. Граф підтвердження підпису

Висновки

1. Використання ізогеній є одним з шляхів забезпечення стійкості до квантового криптоаналізу. Вже існує декілька схем узгодження ключів та електронного підпису на ізогеніях еліптичних кривих.

2. Складність обчислення ізогенії ЕК становить $O(l^3)$, для її зменшення пропонується використання суперсингулярних кривих. Тоді можливо розбити ізогенію великого порядку на композицію ізогеній низького порядку.

3. Додатковим варіантом оптимізації є використання кривих Едвардса, що дозволить збільшити швидкодію ще в чотири рази. Але це вимогає подальшого дослідження на предмет наявності вразливостей при використанні кривих Едвардса в криптосистемах на ізогеніях ЕК.

4. Складність криптоаналізу схем, заснованих на ізогеніях ЕК, становить $O(p^{1/4})$ для класичного комп'ютера і $O(p^{1/6})$ для квантового, що має експоненційний характер.

5. Схема узгодження ключів – класична схема використання ізогеній в системах з відкритим ключем. В цій схемі дотримуються усі вимоги до криптографічних систем на основі ізогеній.

6. Схема електронного підпису дозволяє підтвердити правильність підпису в інтерактивному режимі з підписувачем. Недоліком є ймовірність підтвердження недійсного підпису, щоб запобігти цьому необхідно виконувати повторні перевірки при інших параметрах.

Список літератури: 1. *Reinier Broker*. Constructing supersingular elliptic curves // J. Comb. Number Theory, (3): pp. 269–273, 2009. 2. *Steven D. Galbraith*. Constructing isogenies between elliptic curves over Finite Fields. LMS J. Comput. Math, 2: pp. 118–138 (electronic), 1999. 3. *David Jao and Luca De Feo*. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, PQCrypto, volume 7071 of Lecture Notes in Computer Science, pp. 19–34. Springer, 2011. 4. *Jacques Velu*. Isogenies entre courbes elliptiques. – C. R. Acad. Sci. Paris Ser. A-B,– 273: A238 – A241, 1971. 5. *David Jao, Vladimir Soukharev*. Isogeny-Based Quantum-Resistant Undeniable Signatures. PQCrypto 2014: pp. 160-179. 6. *O. Ahmadi, and R. Granger*, On isogeny classes of Edwards curves over nite elds, J. Number Theory, 132 (6), pp. 1337-1358, (2011).

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 12.09.2016